National University
of computer and emerging sciences

Project Report

Ceaser Cipher

Group Members

1.Muzamil p20-0108/k201887

2.Amanullah p20-0109

Submitted to:

Course Lecturer: **Aashir Mehboob**

Lab Instructor: **Kariz Kamal**

Introduction

Caesar cipher is one of safe tool for protecting any data which will be safe that data can`t be

Accessed by another person the data can be accessed by that person only who knows the key

That data will be in between two guys, One who send data one who receive data

Goal

In Our Program we have encrypted the data (converted plain text into cipher text) so that no one can understand what is written and in this program we also converted this cipher text into plain text (decrypted the encrypted data)

Tools and techniques

Here we have used 3 Function (Procedures) one input proc 2nd one is Display and 3rd is Translate Proc In input proc we got user input data which is converted into cipher text in translate proc and in the last In Display function we displayed the data which is encrypted and decrypted our program will ask key from user at run time.

- ✓ ***Visual studio***
- ✓ ***Window 10***

Code:

```
INCLUDE Irvine32.inc
key=23
bufmax=200
;-----------------------------------------------------------------------------------------------------------------
.data
msg byte "                                    **********WE WARMLY WELCOME YOU *****************",0
msg1 byte "ENTER THE TEXT THAT YOU WANT TO encrypt ",0

msg2 byte "the cipher text of entered message is ",0

msg3 byte "decrypted: ",0

wrong BYTE,"yOU entered wrong key",0

keey BYTE "Enter key for decryption: ",0

buffer byte bufmax+1 DUP (0)

bufsize DWORD ?

;-----------------------------------------------------------------------------------------------------------------

.code

main proc
MOV EDX,OFFSET MSG
call writestring
mov eax,yellow+(blue*16)
call settextcolor
call crlf

call input
call translate
mov edx,offset msg2
call display
call translate
mov edx,offset keey
call writestring
call readdec
cmp eax,key
```

```
call display


jmp l2
l1:
mov edx,OFFSET wrong
call writestring
l2:
call crlf


exit


main endp


;-----------------------------------------------------------------------------------------------------------------


input PROC
pushad         ;Pushes registers on stack

mov eax,(blue*16) ;set the text color
call settextcolor


mov edx,offset msg1

call writestring
call crlf

mov ecx,bufmax
mov edx,offset buffer
call readstring
mov bufsize,eax
```

```
mov edx,offset msg1

call writestring
call crlf

mov ecx,bufmax
mov edx,offset buffer
call readstring
mov bufsize,eax
call crlf
popad
ret
input endp
;-----------------------------------------------------------------------------

display PROC
pushad
call writestring
mov edx,offset buffer
call writestring
call crlf
call crlf
popad
ret
display endp


;-----------------------------------------------------------------------------

translate PROC


pushad
mov ecx,bufsize
mov esi,0
l1:
xor buffer[esi],key
inc esi
```

Output:


**********WE WARMLY WELCOME YOU **********
ENTER THE TEXT THAT YOU WANT TO encrypt
Aman
the cipher text of entered message is: Vzvy
Enter key for decryption: 23
decrypted: decrypted: Aman
Press any key to continue . . .